

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	39340	encrypt\$3 and decrypt\$3	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/07/06 17:06
L2	60586	(encrypt\$3 or decrypt\$3 or encipher\$3 or decipher\$3 or temporary or public or shar\$3 or secret) near6 key	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/07/06 17:08
L3	27199	1 and 2	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/07/06 17:08
L4	4821	(append\$4 or attach\$5) with signature	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/07/06 17:09
L5	2121	3 and 4	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/07/06 17:10
L6	1432	(encrypt\$3 or encipher) with (money or monetary or balance or cash or ecash)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/07/06 17:13
L7	148	5 and 6	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/07/06 17:11
L8	381	(decrypt\$3 or decipher) with (money or monetary or balance or cash or ecash)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/07/06 17:11
L9	69	5 and 8	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/07/06 17:11

EAST Search History

L10	158	7 or 9	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/07/06 17:11
ready (L11)	59	10 and @ad<"19981008"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/07/06 17:15
L12	82948	signature	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/07/06 17:12
L13	10243	3 and 12	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/07/06 17:13
L14	9879	(encrypt\$3 or encipher) with (signature or money or monetary or balance or cash or ecash)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/07/06 17:13
L15	4748	(decrypt\$3 or decipher) with (signature or money or monetary or balance or cash or ecash)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/07/06 17:13
L16	10470	14 or 15	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/07/06 17:13
L17	6431	13 and 16	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/07/06 17:13
L18	463689	(add\$3 or credit) near6 (amount or money or cash or ecash or monetary or balance)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/07/06 17:14
L19	464578	(add\$3 or credit\$3) near6 (amount or money or cash or ecash or monetary or balance)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/07/06 17:14

EAST Search History

L20	1209	17 and 19	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/07/06 17:14
L21	248	20 and @ad<"19981008"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/07/06 17:15
read L22	204	21 not 11	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/07/06 17:15

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	20172	encrypt\$3 and decrypt\$3	US-PGPUB	OR	ON	2006/07/06 17:55
L2	18132	key and signature	US-PGPUB	OR	ON	2006/07/06 17:55
L3	6732	1 and 2	US-PGPUB	OR	ON	2006/07/06 17:55
real L4	36	3 and @ad<"19981008"	US-PGPUB	OR	ON	2006/07/06 17:55

? show files

File 15:ABI/Inform(R) 1971-2006/Jul 06
 (c) 2006 ProQuest Info&Learning
 File 16:Gale Group PROMT(R) 1990-2006/Jul 05
 (c) 2006 The Gale Group
 File 148:Gale Group Trade & Industry DB 1976-2006/Jul 04
 (c)2006 The Gale Group
 File 160:Gale Group PROMT(R) 1972-1989
 (c) 1999 The Gale Group
 File 275:Gale Group Computer DB(TM) 1983-2006/Jul 05
 (c) 2006 The Gale Group
 File 621:Gale Group New Prod.Annou.(R) 1985-2006/Jul 04
 (c) 2006 The Gale Group
 File 9:Business & Industry(R) Jul/1994-2006/Jul 05
 (c) 2006 The Gale Group
 File 20:Dialog Global Reporter 1997-2006/Jul 06
 (c) 2006 Dialog
 File 476:Financial Times Fulltext 1982-2006/Jul 07
 (c) 2006 Financial Times Ltd
 File 610:Business Wire 1999-2006/Jul 06
 (c) 2006 Business Wire.
 File 613:PR Newswire 1999-2006/Jul 06
 (c) 2006 PR Newswire Association Inc
 File 624:McGraw-Hill Publications 1985-2006/Jul 06
 (c) 2006 McGraw-Hill Co. Inc
 File 634:San Jose Mercury Jun 1985-2006/Jul 05
 (c) 2006 San Jose Mercury News
 File 636:Gale Group Newsletter DB(TM) 1987-2006/Jul 05
 (c) 2006 The Gale Group
 File 810:Business Wire 1986-1999/Feb 28
 (c) 1999 Business Wire
 File 813:PR Newswire 1987-1999/Apr 30
 (c) 1999 PR Newswire Association Inc
 File 2:INSPEC 1898-2006/Jun W4
 (c) 2006 Institution of Electrical Engineers
 File 35:Dissertation Abs Online 1861-2006/Jun
 (c) 2006 ProQuest Info&Learning
 File 65:Inside Conferences 1993-2006/Jul 06
 (c) 2006 BLDSC all rts. reserv.
 File 99:Wilson Appl. Sci & Tech Abs 1983-2006/Jun
 (c) 2006 The HW Wilson Co.
 File 256:TecInfoSource 82-2006/Aug
 (c) 2006 Info.Sources Inc
 File 474:New York Times Abs 1969-2006/Jul 05
 (c) 2006 The New York Times
 File 475:Wall Street Journal Abs 1973-2006/Jul 05
 (c) 2006 The New York Times
 File 583:Gale Group Globalbase(TM) 1986-2002/Dec 13
 (c) 2002 The Gale Group

? ds

Set	Items	Description
S1	369097	ENCRYPT???? OR ENCIPHER????
S2	74108	DECRYPT???? OR DECIPHER????
S3	38934044	TEMPORAR???? OR PUBLIC OR SHAR??? OR SECRET? ? OR PRIVATE
S4	8404386	KEY OR KEYS
S5	321473	(S1 OR S2 OR S3) (6N) S4
S6	12449	S1 AND S2 AND S5
S7	15965444	MONEY OR MONETARY OR CASH OR ECASH OR BALANCE? ?
S8	3138	(S1 OR S2) (10N) S7

read S9 259 S6 AND S8
S10 726206 SIGNATURE? ?
S11 62 S9 AND S10
S12 46 S11 NOT PY>1998
S13 40 RD (unique items)

see the order placed.

13/3,AB/26 (Item 4 from file: 275)

DIALOG(R) File 275:Gale Group Computer DB(TM)

(c) 2006 The Gale Group. All rts. reserv.

02104494 SUPPLIER NUMBER: 19758223 (USE FORMAT 7 OR 9 FOR FULL TEXT)

Cracking the code: experimenting with encryption and Java. (Technology Tutorial) (Tutorial)

Dragan, Rich

Computer Shopper, v16, n10, p603(3)

Oct, 1997

DOCUMENT TYPE: Tutorial ISSN: 0886-0556 LANGUAGE: English

RECORD TYPE: Fulltext; Abstract

WORD COUNT: 1892 LINE COUNT: 00147

ABSTRACT: A guide to data **encryption** using the Java language is presented. Cryptography is based on the principle of a one-way function, which converts data so that it cannot be reverse-engineered. Large prime numbers and other areas of higher math are usually the basic sources for such functions. **Public - key** cryptography is an approach that uses a set of asymmetrical keys, one available to anyone and the other known only to a single user. The DES standard, which uses a symmetrical 56-bit key, is still widely accepted because it offers over 72 trillion **keys** .

Encryption is difficult to crack with brute force, but longer keys and more powerful algorithms are needed to ensure security as computing power increases. RSA Data Security's RSA **encryption** algorithm is widely used today, especially on the Web. Cryptanalysis involves breaking codes to see if **encryption** algorithms are sound. A sample Java program demonstrating cryptography is presented.

13/3,AB/27 (Item 5 from file: 275)

DIALOG(R) File 275:Gale Group Computer DB(TM)

(c) 2006 The Gale Group. All rts. reserv.

02090579 SUPPLIER NUMBER: 19662963 (USE FORMAT 7 OR 9 FOR FULL TEXT)

Give your site some credit: preparing your Web site to handle credit-card transactions. (includes related article on do-it-yourself commerce sites) (Internet/Web/Online Service Information) (Tutorial)

Tadger, Rivka

Computer Shopper, v16, n9, p618(6)

Sep, 1997

DOCUMENT TYPE: Tutorial ISSN: 0886-0556 LANGUAGE: English

RECORD TYPE: Fulltext; Abstract

WORD COUNT: 6002 LINE COUNT: 00471

ABSTRACT: More and more Web-site developers are creating interactive storefronts, but moving into electronic commerce is a serious undertaking that demands careful planning. About half of US businesses with credit-enabled Web sites outsource the transaction capability, something that can be done even if the rest of the site resides in-house. A third-party service bureau can handle large volumes of transactions and provide tight security. Most bureaus charge \$100 to \$500 per month plus per-transaction fees of 3 to 15 percent. The core issue in Web commerce is not company size but how many products are sold on the Web. Developers of online commerce sites should always be aware of technology fundamentals and

the fact that adding credit-card transactions is first and foremost a banking function. Web-commerce server software such as that available from Microsoft, Internet Factory and Mercantec handles product IDs, pricing and transaction **encryption**. Adding security is partly a public-relations issue.

13/3,AB/28 (Item 6 from file: 275)

DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2006 The Gale Group. All rts. reserv.

01861490 SUPPLIER NUMBER: 17433056 (USE FORMAT 7 OR 9 FOR FULL TEXT)
On-line Lucre. (securing commercial transactions on the Web) (includes related articles) (Industry Trend or Event)

Richardson, Robert
LAN Magazine, p101(5)
Oct, 1995

ISSN: 1069-5621 LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 4075 LINE COUNT: 00326

ABSTRACT: As the Internet and World Wide Web turn into increasingly commercial venues, the security of financial transactions becomes paramount. Using the Netscape Navigator Web browser, buyer and vendor benefit from a private channel that results from a protocol that has been proposed as an industry standard, the Secure Socket Layer (SSL). This protocol builds and maintains **encrypted** connections between buyers and vendors. It is not specific to the Web, and similar connections could occur elsewhere on the Net. Another means of security, Enterprise Integration Technologies' (EIT) S-HTTP, appeared before Netscape's to protect Web users.

13/3,AB/29 (Item 7 from file: 275)

DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2006 The Gale Group. All rts. reserv.

01801703 SUPPLIER NUMBER: 17162680 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Toward electronic money: some Internet experiments. (includes related articles on RSA's public - key encryption and on smart cards for digital money)

Dyson, Peter E.
Seybold Report on Desktop Publishing, v9, n10, p3(9)
June 10, 1995

ISSN: 0889-9762 LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 6493 LINE COUNT: 00607

13/3,AB/30 (Item 8 from file: 275)

DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2006 The Gale Group. All rts. reserv.

01600581 SUPPLIER NUMBER: 13734522 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Stump the cipher punks. (data encryption for network security) (includes related articles on the Data Encryption Standard, encryption algorithms and a hypothetical code-breaking computer)

Hyatt, Glenn
LAN Magazine, v8, n6, p93(6)
June, 1993

ISSN: 0898-0012 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 3348 LINE COUNT: 00260

ABSTRACT: Sensitive data on a network is vulnerable to unauthorized access, but this can be minimized through effective use of data **encryption**. Running the original file through an **encryption** algorithm results in a scrambled file that may only be decoded with a specific character or numeric string, called a key, which corresponds to the original algorithm. Symmetric **encryption** uses the same **key** for **encryption** and **decryption**, while asymmetric **encryption** uses different **keys** for each process. 'Public key algorithms' are very useful in that they require two **keys** for data **encryption** and are especially necessary on a network because data is 'broadcast' rather than 'narrowcast' over these enterprises. A server will send a requested file to every node on the LAN, with the assumption that it will be accessible only by the requesting user. The managerial decision to implement **encryption** should include the value of the network's data, the cost of implementation, the effectiveness of the chosen **encryption** method and the likelihood of break-in attempts. The **encryption** capabilities of various network management systems are discussed.

13/3,AB/31 (Item 9 from file: 275)

DIALOG(R) File 275:Gale Group Computer DB(TM)

(c) 2006 The Gale Group. All rts. reserv.

01548046 SUPPLIER NUMBER: 12937984 (USE FORMAT 7 OR 9 FOR FULL TEXT)

Comments on cryptography. (ACM Forum) (Letter to the Editor)

Knowles, Brad; Schlafly, Roger; Schultz, Grant D.; Zelvin, Lynn; Heckel, Paul; Yoches, E. Robert

Communications of the ACM, v35, n11, p19(5)

Nov, 1992

DOCUMENT TYPE: Letter to the Editor

ISSN: 0001-0782

LANGUAGE:

ENGLISH

RECORD TYPE: FULLTEXT

WORD COUNT: 4128 LINE COUNT: 00325

13/3,AB/32 (Item 10 from file: 275)

DIALOG(R) File 275:Gale Group Computer DB(TM)

(c) 2006 The Gale Group. All rts. reserv.

01438721 SUPPLIER NUMBER: 10974982 (USE FORMAT 7 OR 9 FOR FULL TEXT)

Accusations fly as NIST security standard challenged. (National Institute of Standards and Technology)

McCormick, John

Newsbytes, NEW07100027

July 10, 1991

LANGUAGE: ENGLISH

RECORD TYPE: FULLTEXT

WORD COUNT: 876 LINE COUNT: 00066

13/3,AB/33 (Item 11 from file: 275)

DIALOG(R) File 275:Gale Group Computer DB(TM)

(c) 2006 The Gale Group. All rts. reserv.

01213399 SUPPLIER NUMBER: 04683843 (USE FORMAT 7 OR 9 FOR FULL TEXT)

Network applications are adding encryption. (connectivity section)

Kramer, Matt

PC Week, v4, n9, pC7(1)

March 3, 1987

ISSN: 0740-1604

LANGUAGE: ENGLISH

RECORD TYPE: FULLTEXT; ABSTRACT

WORD COUNT: 1273

LINE COUNT: 00101

ABSTRACT: Network applications require a different form of security than single-user applications because of the use of a common file server. This means the data cannot be locked away as is done on single-user systems. The passwords used to protect file-server data can be bypassed by utility packages. Several different approaches are being used by software developers and hardware manufacturers to protect data on networks.

Microsoft has added **encryption** to its MultiPlan spreadsheet that requires a key be used to read the data. Ashton-Tate's dBASE III Plus provides **encryption** through the Protect utility included. RSA Data Security uses a data **encryption** method that uses different **keys** for **encryption** and **decryption**. This allows the **encryption** **key** to be made **public** as long as the **decryption** **key** is kept **private**. Micronyx is developing an **encryption** board for workstations and file servers that requires users to insert a computer chip into the board to **decrypt** the data. Other network data **encryption** plans of network hardware and software developers are described.

13/3,AB/34 (Item 1 from file: 20)

DIALOG(R)File 20:Dialog Global Reporter

(c) 2006 Dialog. All rts. reserv.

02950336

RPK Security's "SafeCracker Challenge" Invites Users to "Break" RPK
Encryptonite Engine and Win \$10,000

BUSINESS WIRE

September 28, 1998

JOURNAL CODE: WBWE

LANGUAGE: English

RECORD TYPE: FULLTEXT

WORD COUNT: 363

SAN FRANCISCO--(BUSINESS WIRE)--Sept. 28, 1998--RPK Security, Inc., a technology leader in fast **public key encryption**, announced today the "SafeCracker Challenge", a contest offering US\$10,000 to the first person who breaks the technology behind the company's uniquely fast **public key** cryptosystem, RPK Encryptonite Engine. In order to receive the **cash** reward, participants must download the **encrypted** test document and test **public key** from RPK Security's website, www.rpkusa.com, and then submit via email the **private key** that corresponds to the current test **public key**, or the correctly **decrypted** test document. "We're launching the SafeCracker Challenge to demonstrate that the RPK Encryptonite Engine provides the most secure, fast and flexible **public key** system on the market today," said Jack Oswald, president and CEO of RPK Security. "Recently patented in New Zealand and the US, the technology behind the RPK Encryptonite Engine is based on the same mathematics as Diffie-Hellman Key Exchange, a widely used algorithm for creating secure network-based communications systems, and is highly respected by security experts." The RPK Encryptonite Engine is a uniquely fast **public key** algorithm for **encryption**, authentication and digital **signatures**. It offers a combination of the benefits of commonly used **public key** systems (ease of **key** management, authentication and digital **signatures**) and the high performance characteristics of commonly used symmetric or "**secret key**" systems. Developed outside of the U.S., the RPK Encryptonite Engine is

available globally with strong **encryption**, unlike competing products that are restricted by U.S. export regulations. ABOUT RPK SECURITY Founded in 1995, RPK Security, Inc. is a technology leader in fast **public key** cryptography. Its flagship RPK Encryptonite(TM) Engine, a uniquely fast and strong **public key encryption** technology, is available worldwide in custom hardware and software toolkits on multiple platforms. Developed from widely accepted security mathematics and techniques, the RPK Encryptonite Engine is easily embedded into new and existing hardware and software applications. RPK's cryptographic research and product development is based in New Zealand, Switzerland and the U.K., with worldwide sales and marketing operations in San Francisco, CA. Visit RPK's website at www.rpkusa.com or call 212/488-9891. CONTACT: Nadel Phelan, Inc. Paula Miller, 408/439-5570 x277 paulam@nadelphelan.com or RPK Security Inc. Lyn Oswald, 212/488-9891 lynoswald@rpkusa.com 10:02 EDT SEPTEMBER 28, 1998

13/3,AB/35 (Item 2 from file: 20)

DIALOG(R)File 20:Dialog Global Reporter
(c) 2006 Dialog. All rts. reserv.

01469118

Business This Week: Is your money safe from super-highwaymen?: In the age of the ATM and the Net, banks face the old problem - how much to tell; how much to hide

EOIN LICKEN

IRISH TIMES, p59

April 24, 1998

JOURNAL CODE: FIRT LANGUAGE: English RECORD TYPE: FULLTEXT

WORD COUNT: 680

The current controversy surrounding banking has shown the importance of trust between a bank and its customers. One part of that trust has always been the belief that money is secure in a bank that nobody else can access your account but as electronic banking grows, how can people know that this is still the case? In the information age, how safe is your money from information super-highway robbers?

Banks have long been in a dilemma over how much of their security to reveal. From the earliest days of safes, shutters and bars on windows, banks have had to show enough security to reassure customers, while not revealing too much of their practices to potential bank robbers. In the age of electronic banking, via ATMs, telephones, and the Internet, the same dilemma holds: how much to tell, how much to hide?

13/3,AB/36 (Item 1 from file: 476)

DIALOG(R)File 476:Financial Times Fulltext

(c) 2006 Financial Times Ltd. All rts. reserv.

0009585048 B0IL3ATACNFT

INSIDE TRACK: The key to building trust in e-commerce: INFORMATION

TECHNOLOGY INTERNET SECURITY: Public key infrastructures will give potential online customers the confidence they demand, writes Alan Stewart

ALAN STEWART

Financial Times, London Edition 1 ED, P 9

Wednesday, December 30, 1998

DOCUMENT TYPE: Features; NEWSPAPER LANGUAGE: ENGLISH RECORD TYPE:

FULLTEXT

Word Count: 1,054

ABSTRACT:

Support Services, Information Technology.

13/3,AB/37 (Item 1 from file: 636)

DIALOG(R) File 636:Gale Group Newsletter DB(TM)
(c) 2006 The Gale Group. All rts. reserv.

03154470 Supplier Number: 46458044

DTI: Government sets out proposals for encryption on public telecommunications networks

M2 Presswire, pN/A

June 11, 1996

Language: English Record Type: Fulltext

Document Type: Newswire; Trade

Word Count: 1869

13/3,AB/38 (Item 2 from file: 636)

DIALOG(R) File 636:Gale Group Newsletter DB(TM)
(c) 2006 The Gale Group. All rts. reserv.

02334383 Supplier Number: 44560889

US DoD TO TEST NEW E-MAIL SECURITY PRODUCTS

Computer Fraud & Security Bulletin, pN/A

April, 1994

Language: English Record Type: Fulltext

Document Type: Newsletter; Trade

Word Count: 1606

13/3,AB/39 (Item 3 from file: 636)

DIALOG(R) File 636:Gale Group Newsletter DB(TM)
(c) 2006 The Gale Group. All rts. reserv.

02226522 Supplier Number: 44239037

FACING SECURITY, CONTROL ISSUES CRITICAL FOR EFT/EDI

Corporate EFT Report, v13, n22, pN/A

Nov 17, 1993

Language: English Record Type: Fulltext

Document Type: Newsletter; Trade

Word Count: 728

13/3,AB/40 (Item 4 from file: 636)

DIALOG(R) File 636:Gale Group Newsletter DB(TM)
(c) 2006 The Gale Group. All rts. reserv.

01533483 Supplier Number: 42212462

ACCUSATIONS FLY AS NIST SECURITY STANDARD CHALLENGED 07/10/91

Newsbytes, pN/A

July 10, 1991

Language: English Record Type: Fulltext

Document Type: Newswire; General Trade

Word Count: 817

?

13/3,AB/1 (Item 1 from file: 15)

DIALOG(R)File 15:ABI/Inform(R)

(c) 2006 ProQuest Info&Learning. All rts. reserv.

02363346 117541231

Electronic commerce - would, could and should you use current Internet payment mechanisms?

Buck, S. Peter

Internet Research v6n2/3 PP: 5-18 1996 ISSN: 1066-2243 JRNL CODE: NTRS

WORD COUNT: 7209

ABSTRACT: It is suggested that the discussion of online payments, while ultimately being a key issue for the future information SuperHighway, is as significant now as it ever will be. The explosive increase in the use of the Internet has seen the emergence of commercial services and pressures previously restricted to Compuserve and the like. Many predictions see this burgeoning electronic marketplace becoming a significant component of the world economy. However, this can only happen once two key problems have been addressed, namely, protecting property rights and making payments. This has led to a frantic battle for payment mechanisms that can provide the new medium with the means of conduction transactions. The key commercial requirements that successful use of the Internet will impose on a payment mechanism are identified. Each of these mechanisms are evaluated against the requirements to determine which (if any) are really suitable for electronic commerce.

13/3,AB/2 (Item 2 from file: 15)

DIALOG(R)File 15:ABI/Inform(R)

(c) 2006 ProQuest Info&Learning. All rts. reserv.

01738302 03-89292

Protect yourself

Krishna, Arvind

Inform v12n10 PP: 26-29 Nov 1998 ISSN: 0892-3876 JRNL CODE: IFN

WORD COUNT: 2524

ABSTRACT: E-commerce is really an umbrella term for technologies, processes, and management techniques that automate business transactions through paperless mechanisms. Implementing appropriate security countermeasures, and establishing proper business controls and a legal framework can mitigate the risks inherent in Internet E-Commerce. In general, security vulnerabilities can be divided into 2 major categories: user authorization and data/transaction security. User authorization controls deal with services, such as user identification, authentication, and access controls. Access control refers to restricting access to the resources of an automated information system to only authorized users, programs, processors, and systems. A firewall is the most widely used security tool that enforces a network access control policy by monitoring all traffic going to or from the network. **Public - key encryption**, digital **signatures**, digital certificates, and **public - key** infrastructure are also discussed.

13/3,AB/3 (Item 3 from file: 15)

DIALOG(R)File 15:ABI/Inform(R)

(c) 2006 ProQuest Info&Learning. All rts. reserv.

01555295 02-06284

CD DVD piracy: The replicator, the user, and the technology

Block, Debbie Galante

EMedia Professional v10n12 PP: 92-107 Dec 1997 ISSN: 1090-946X

JRNL CODE: LDP

WORD COUNT: 6432

ABSTRACT: Two opposing schools of thought fuel the debate over combating software piracy. One camp maintains that anti-piracy technologies like **encryption** are necessary deterrents, while the opposing view holds that any anti-piracy technology is useless and that pirates will take their share regardless of the methods used. Publishers are beginning to demand proof that anti-piracy technologies work without turning off legitimate users. Instead, what exists so far are descriptions of what today's anti-piracy technologies do, how they work, how they are positioned, and how their developers and early adopters see these hardware and software technologies combating the genuine problem of software piracy, especially as piracy's prospects grow increasingly intriguing in the lucrative and largely uncharted world of DVD. One way CD replicators are playing a key role in making sure legitimate CDs get into the stores is by applying Source Identification Codes to the discs they press. For software protection, a small amount of code is added to installation files, which works with an added layer of one of several proprietary polymers on the CD-ROM or DVD-ROM media.

13/3,AB/4 (Item 4 from file: 15)

DIALOG(R)File 15:ABI/Inform(R)

(c) 2006 ProQuest Info&Learning. All rts. reserv.

01547217 01-98205

The future of Internet EC

Anonymous

Internal Auditor v54n6 PP: 32-33 Dec 1997 ISSN: 0020-5745 JRNL CODE:

IAU

WORD COUNT: 965

ABSTRACT: The on-line store concept is in its infancy, but progress is being made in 2 technologies - electronic **cash** and **public key encryption** - that should enable the exponential growth of trade on the Internet. To properly audit electronic commerce via the Internet, auditors should be exposed to these 2 enabling technologies.

13/3,AB/5 (Item 5 from file: 15)

DIALOG(R)File 15:ABI/Inform(R)

(c) 2006 ProQuest Info&Learning. All rts. reserv.

01386565 00-37552

Making payments on the Internet

McAndrews, James J

Business Review (Federal Reserve Bank of Philadelphia) PP: 3-14 Jan/Feb

1997 ISSN: 0007-7011 JRNL CODE: FRB

WORD COUNT: 5504

ABSTRACT: To flourish as a marketplace, the Internet needs a means of payment. The challenge is to devise ways to protect against theft while conveying payment information that is recognized as authentic. Most

payment services on the Internet use some form of **public key / private key encryption**, but others safeguard financial information in other ways. With a trusted-3rd-party method of payment, a customer authorizes the trusted 3rd party to make payments on his/her behalf. Another method of payment is digital cash, which is stored on a computer's hard disk and is electronically transferred to a payee. Digital cash systems typically propose to prevent counterfeiting by virtue of the issuer's digital **signature** on the digital cash, which verifies its authenticity. For the proposed payment systems, issues such as consumer protection, disclosure and assignment of participant liability and privacy are being addressed by regulators and law makers. Recently, the Federal Reserve suggested that stored-value-cards that can store no more than \$100 be exempted from the provision of Regulation E, which governs many conventional electronic methods of payment.

13/3,AB/6 (Item 6 from file: 15)

DIALOG(R)File 15:ABI/Inform(R)

(c) 2006 ProQuest Info&Learning. All rts. reserv.

01223259 98-72654

Perils and pitfalls of practical cybercommerce

Borenstein, Nathaniel S

Communications of the ACM v39n6 PP: 36-44 Jun 1996 ISSN: 0001-0782

JRNL CODE: ACM

WORD COUNT: 6681

ABSTRACT: First Virtual Holdings was formed in early 1994 to facilitate Internet commerce. The first product offering from First Virtual was an Internet payment system, which was developed quietly and publicly announced as a fully operational open Internet service on October 15, 1994. Unlike many other would-be players in the field of Internet commerce, First Virtual chose to announce its payment system only after it was fully operational. In its first year of operation, the company has experienced exponential growth, and it has gained substantial experience with and insight into the nature of Internet commerce. The lessons learned by the First Virtual team during a year of actual operation of an Internet commerce system, as well as what the team sees as prospects for the future, are discussed.

13/3,AB/7 (Item 7 from file: 15)

DIALOG(R)File 15:ABI/Inform(R)

(c) 2006 ProQuest Info&Learning. All rts. reserv.

01155725 98-05120

Showdown over e-cash

Anderson, Howard

Upside v8n1 PP: 24-36 Jan 1996 ISSN: 1052-0341 JRNL CODE: UPS

WORD COUNT: 4930

ABSTRACT: The whole structure of traditional money is built on faith - just as e-money will have to be. As long as a trusted agent can guarantee that the information is valid, that the funds are really there, and that the buyer is the person he or she purports to be, there is no reason why funds cannot be moved like e-mail is. In a new e-cash world, a fiduciary's role will change. Functionally, AT&T's credit card business, Bank of America's

1,000 branches, and the Microsoft network are exactly the same - transaction-heavy processing networks. Banks are worried, because they realize intuitively that the functions they have performed are soon to be performed by their customers. When entities other than the central bank lends money to other banks - thereby increasing or decreasing interest rates to control economic activity - the power of any central government is diminished. Bankers are scared because their real competition is the likes of AT&T and Microsoft. E-money is going to drive transactions, and transactions are going to drive the Internet.

13/3,AB/8 (Item 8 from file: 15)
 DIALOG(R)File 15:ABI/Inform(R)
 (c) 2006 ProQuest Info&Learning. All rts. reserv.

01124373 97-73767

Payments on the 'Net? How many? How safe?

Lunt, Penny
 ABA Banking Journal v87n11 PP: 46-54 Nov 1995 ISSN: 0194-5947
 JRNL CODE: BNK
 WORD COUNT: 3156

ABSTRACT: Research firm Killen & Associates estimates that there will be 7 billion Internet payments made in the year 2000 and 17 billion in 2005. Assuming a typical transaction fee of \$1.50, the organizations that dominate Internet commerce will take in \$11 billion in 2000 and \$26 billion in 2005. Both nonbanks and banks have a head start in the embryonic Internet retail payment system, which so far includes only credit card and off-line debit card payments. The first company to provide secure credit card transactions over the Internet, First Virtual Holdings, Inc., has been growing 15% a week since February, 1995. Banks need to form a policymaking entity that makes rules for Internet commerce. Michael Karlin of Security First Network Bank warns that the banking industry has given away profitable niches before, and it is possible that it could give this one away.

13/3,AB/9 (Item 9 from file: 15)
 DIALOG(R)File 15:ABI/Inform(R)
 (c) 2006 ProQuest Info&Learning. All rts. reserv.

01119712 97-69106

Secrecy and authenticity

Balon, Brett
 Records Management Quarterly v29n4 PP: 24-31 Oct 1995 ISSN: 1050-2343
 JRNL CODE: RMQ
 WORD COUNT: 5866

ABSTRACT: Records managers should be aware of the continuing debate about the Clipper/Skipjack/Capstone **encryption** schemes and the needs of law enforcement and national security versus the right to privacy and freedom from government interference. They should also be aware of the **encryption** schemes in use by their company, the benefits and drawbacks of various methods, and be prepared to make recommendations. Records managers should be aware of the rules governing **encryption** in other countries and consider its impact on recordkeeping, especially in foreign subsidiaries. Computer and communications manufacturers that incorporate the chipset into their products can expect that export sales will drop if their clients know that these **encryption** chips are included. Whether US clients will want

to have these chipsets in their communications equipment is doubtful. Whether the US federal government can make US communications firms inside and outside the US use the Clipper chipset and incorporate it into their devices is up in the air.

13/3,AB/10 (Item 10 from file: 15)

DIALOG(R)File 15:ABI/Inform(R)

(c) 2006 ProQuest Info&Learning. All rts. reserv.

01053397 97-02791

The information highway and you

Stahl, David

America's Community Banker v4n6 PP: 29-35 Jun 1995 ISSN: 1082-7919

JRNL CODE: SLN

WORD COUNT: 4188

ABSTRACT: All kinds of neat things, along with a variety of detritus, can be found on the Internet. It is the World Wide Web (WWW) that serves as the epicenter for much of the excitement surrounding the Internet. The Web, which combines graphics with text, permits browsers to obtain more detailed information by using hypertext jumps. Such jumps enable a person to switch quickly to a new page or, to surf the Internet. Thus far, a number of companies have established Web pages. Financial institutions are using such pages to post their interest rates. Salem Five Cents Savings Bank (Massachusetts) opened its first "virtual branch" in April 1995, permitting customers to open savings and checking accounts, or purchase a CD.

13/3,AB/11 (Item 11 from file: 15)

DIALOG(R)File 15:ABI/Inform(R)

(c) 2006 ProQuest Info&Learning. All rts. reserv.

00911907 95-61299

Cryptography policy

Hoffman, Lance J; Ali, Faraz A; Heckler, Steven L; Huybrechts, Ann

Communications of the ACM v37n9 PP: 109-117 Sep 1994 ISSN: 0001-0782

JRNL CODE: ACM

WORD COUNT: 7676

ABSTRACT: The availability and the desirability of **encrypting** some communications is just starting to be generally recognized by US business, and the **encryption** market is just now beginning to emerge as a significant part of the computer security market. As a result, a debate about the proper balance of national security, law enforcement and personal freedom has been initiated. Law enforcement and national security agencies would like to maintain tight control over civilian **encryption** technologies, while industry and individual and property rights advocates fight to expand their ability to distribute and use cryptographic products as they please. Trends in **encryption** technology and policy are analyzed. These trends are divided into 4 areas: 1. technology, 2. market analysis, 3. export controls, and 4. public policy issues. Four scenarios based on these trends can be envisioned: 1. complete decontrol of cryptography, 2. domestic decontrol of cryptography with export regulations, 3. voluntary escrowed **encryption**, and 4. mandatory escrowed **encryption**.

13/3,AB/12 (Item 1 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2006 The Gale Group. All rts. reserv.

05096081 Supplier Number: 47482099
New tools for the trade II
InfoWorld, p92
June 23, 1997
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 6536

13/3,AB/13 (Item 2 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2006 The Gale Group. All rts. reserv.

04849802 Supplier Number: 47134480
**Smartcards: Motorola to supply chips for Visa Cash stored-value card; U.K.
test site for global smartcard initiative that will reduce need for cash
for small-value transactions**
EDGE: Work-Group Computing Report, pN/A
Feb 17, 1997
Language: English Record Type: Fulltext
Document Type: Newsletter; Trade
Word Count: 999

13/3,AB/14 (Item 3 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2006 The Gale Group. All rts. reserv.

04528971 Supplier Number: 46654196
**Buying data bit by bit with microcash; New technology lets Internet users
pay as they go**
PC Week, pN03
August 26, 1996
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Tabloid; General Trade
Word Count: 1671

13/3,AB/15 (Item 1 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2006 The Gale Group. All rts. reserv.

0019712554 SUPPLIER NUMBER: 53353930 (USE FORMAT 7 OR 9 FOR FULL
TEXT)
MORGAN COLE: Signatures go hi-tech.
M2 Presswire, NA
Dec 4, 1998
LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 782 LINE COUNT: 00066

13/3,AB/16 (Item 2 from file: 148)

DIALOG(R) File 148:Gale Group Trade & Industry DB
(c)2006 The Gale Group. All rts. reserv.

10036457 SUPPLIER NUMBER: 20332297 (USE FORMAT 7 OR 9 FOR FULL TEXT)

Electronic commerce: can internal auditors help to mitigate the risks?
(includes related articles on electronic commerce and Internet
commerce) (Cover Story)

Stone, William A.

Internal Auditor, v54, n6, p26(9)

Dec, 1997

DOCUMENT TYPE: Cover Story

ISSN: 0020-5745

LANGUAGE: English

RECORD TYPE: Fulltext; Abstract

WORD COUNT: 5481 LINE COUNT: 00455

ABSTRACT: The emergence of electronic commerce (EC) is resulting in significant shifts in the internal auditing profession. Internal auditors can prepare for the inevitable changes by learning the mechanics and risks involved in two of the most common forms of EC, namely electronic data interchange (EDI) and online buying and selling. This understanding should help them effectively examine the EC operation of their clients. When evaluating EDI, internal auditors have to consider several factors, including, security, training and education, audit trail, production controls, communication controls, environmental controls, error detection and correction, and process monitoring. Aside from EDI, internal auditors are also required to familiarize themselves with direct selling and purchasing via the Internet. The same variables as those considered in EDI should be addressed in network transactions although several additional factors should be examined.

13/3,AB/17 (Item 3 from file: 148)

DIALOG(R) File 148:Gale Group Trade & Industry DB
(c)2006 The Gale Group. All rts. reserv.

10018811 SUPPLIER NUMBER: 20006288 (USE FORMAT 7 OR 9 FOR FULL TEXT)

CD DVD piracy: the replicator, the user, and the technology. (includes related articles)

Block, Debbie Galante

EMedia Professional, v10, n12, p92(13)

Dec, 1997

ISSN: 1090-946X

LANGUAGE: English

RECORD TYPE: Fulltext; Abstract

WORD COUNT: 7534 LINE COUNT: 00585

ABSTRACT: The exact economic toll of software piracy on corporate profits in the US is unknown. While one group of individuals believes software piracy should be combatted with data **encryption** technology, another group of individuals believes anti-piracy methods are useless. There are several companies developing anti-piracy methods with each touting its method as the best. Source Identification Codes ensure that legitimate replicated compact discs are available at retail outlets. Each replicator has its own code. Other methods are available to protect software and hardware.

13/3,AB/18 (Item 4 from file: 148)

DIALOG(R) File 148:Gale Group Trade & Industry DB
(c)2006 The Gale Group. All rts. reserv.

09646866 SUPPLIER NUMBER: 17934224 (USE FORMAT 7 OR 9 FOR FULL TEXT)

Smart cards: trained for security. (includes related articles) (Cover Story)

Gallant, John
 EDN, v40, n24, p34(6)
 Nov 23, 1995
 DOCUMENT TYPE: Cover Story ISSN: 0012-7515 LANGUAGE: English
 RECORD TYPE: Fulltext; Abstract
 WORD COUNT: 2451 LINE COUNT: 00195

ABSTRACT: A growing number of banks and merchandisers in the US are using smart cards to provide better services to their customers. These cards feature integrated circuits with **encryption** capabilities that ensure data security and permit on-line transactions. Among the firms which are taking advantage of the growing demand for smart cards are Motorola Inc. and Hitachi Ltd.

13/3,AB/19 (Item 5 from file: 148)
 DIALOG(R)File 148:Gale Group Trade & Industry DB
 (c)2006 The Gale Group. All rts. reserv.

09474579 SUPPLIER NUMBER: 19394751 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Smartcards: Motorola to supply chips for Visa Cash stored-value card; U.K. test site for global smartcard initiative that will reduce need for cash for small-value transactions. (Company Business and Marketing)
 EDGE: Work-Group Computing Report, v8, p28(1)
 Feb 17, 1997
 LANGUAGE: English RECORD TYPE: Fulltext
 WORD COUNT: 1075 LINE COUNT: 00090

13/3,AB/20 (Item 6 from file: 148)
 DIALOG(R)File 148:Gale Group Trade & Industry DB
 (c)2006 The Gale Group. All rts. reserv.

09345122 SUPPLIER NUMBER: 19197877 (USE FORMAT 7 OR 9 FOR FULL TEXT)
IRE Subsidiary Introduces Highly Secure Frame Relay Encryptor for Computer Transmissions; Both 128-bit and DES Algorithms are Offered
 PR Newswire, p312NYW055
 March 12, 1997
 LANGUAGE: English RECORD TYPE: Fulltext
 WORD COUNT: 727 LINE COUNT: 00065

13/3,AB/21 (Item 7 from file: 148)
 DIALOG(R)File 148:Gale Group Trade & Industry DB
 (c)2006 The Gale Group. All rts. reserv.

08940768 SUPPLIER NUMBER: 18624714 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Buying data bit by bit with microcash: new technology lets Internet users pay as they go. (digital cash systems) (includes a related article on Pacific Internet's WebCube Internet server) (PC Week Netweek) (Internet/Web/Online Service Information)
 Kosiur, Dave
 PC Week, v13, n34, pN3(2)
 August 26, 1996
 ISSN: 0740-1604 LANGUAGE: English RECORD TYPE: Fulltext; Abstract
 WORD COUNT: 1794 LINE COUNT: 00144

ABSTRACT: Microcash is a subset of digital cash that lets vendors charge

very small amounts for Web content. Microcash systems are intended primarily for traditional print publishers looking for ways to charge for electronic versions of the information they provide in print form, and self publishers who want to use the Web to provide small groups of users with specialized content. All forms of digital cash involve a broker between the customer and merchant who verifies that funds are available and transfers the appropriate amount to the merchant's account. DigiCash and other digital cash systems issue 'money' that lets users function anonymously and without credit cards if they wish. The **money** is in the form of scrip or tokens and is **encrypted** for transmission between buyer and receiver. The vendor cashes the tokens in for real money, usually in large batch sums. Questions of security remain to be addressed.

13/3,AB/22 (Item 8 from file: 148)

DIALOG(R) File 148:Gale Group Trade & Industry DB
(c)2006 The Gale Group. All rts. reserv.

08361665 SUPPLIER NUMBER: 17722192 (USE FORMAT 7 OR 9 FOR FULL TEXT)

Payments on the 'Net: How many? How safe? (includes articles on the Internet's security, Internet jargon) (Retail Payment System)

Lunt, Penny

ABA Banking Journal, v87, n11, p46(6)

Nov, 1995

ISSN: 0194-5947 LANGUAGE: English RECORD TYPE: Fulltext; Abstract

WORD COUNT: 3340 LINE COUNT: 00268

ABSTRACT: Banks need to take an aggressive role in payment processing over the Internet, or nonbank enterprises will quickly take over that share of the marketplace. Currently, consumers are using credit cards to make purchases over the Internet, and security risks and questions remain in the news. It is likely that credit card companies and other telecommunications companies will soon be supporting electronic payments. Various types of software are being developed to enable simpler transactions to occur without problems.

13/3,AB/23 (Item 1 from file: 275)

DIALOG(R) File 275:Gale Group Computer DB(TM)
(c) 2006 The Gale Group. All rts. reserv.

02192361 SUPPLIER NUMBER: 19690415 (USE FORMAT 7 OR 9 FOR FULL TEXT)

The five fingers of E-mail doom. (network security issues) (Industry Trend or Event)

Power, Richard; Farrow, Rik

Network, v12, n9, p125(2)

Sep, 1997

ISSN: 0142-2383 LANGUAGE: English RECORD TYPE: Fulltext; Abstract

WORD COUNT: 2070 LINE COUNT: 00164

ABSTRACT: E-mail is a convenient, fast, economical and powerful communications tool, but can create serious network security holes. Five common types of threats are spying, spoofing, denial of service, macrovirus proliferation and exposure to civil or criminal liability. A poorly administered node can be compromised by hackers, or an attacker could use a sniffer to filter mail addressed to the server. E-mail forgery compromises the integrity of users' messages, and **encrypted** messages can draw too much attention. Those selecting a cryptographic product should avoid proprietary algorithms. Denial of service attacks include bombing mailboxes

with large numbers of messages. and clogging servers with false traffic. Virus incidents are increasingly common and involve the hiding of virus code in mail attachments. Many employee mail hacking efforts and management errors have ended up in court, damaging a company's image.

13/3,AB/24 (Item 2 from file: 275)

DIALOG(R) File 275:Gale Group Computer DB(TM)

(c) 2006 The Gale Group. All rts. reserv.

02128497 SUPPLIER NUMBER: 20039024 (USE FORMAT 7 OR 9 FOR FULL TEXT)

What can E-money do for me? (Technology Information)

Steinke, Steve

Network, v12, n13, p71(5)

Dec, 1997

LANGUAGE: English RECORD TYPE: Fulltext; Abstract

WORD COUNT: 4169 LINE COUNT: 00346

ABSTRACT: Electronic commerce transactions over the Internet will probably continue to grow in popularity, while some form of digital cash is increasingly used for small and disreputable transactions. Money has, over the last couple of centuries, become increasingly abstracted from the metallic commodities from which it was derived. Over 70% of the monetary measure, known as M1, exists only as entries in bank computers. The Internet changes current electronic transactions very little, but it does open up certain privacy and traceability concerns. On the consumer side, users want assurance of a certain level of anonymity to protect them from potential direct marketing and governmental abuses. On the other hand, total anonymity would create a potential playground for various malefactors. Digital cash provides the ability to make small transactions anonymously, while Internet-based credit card transactions can provide security and a level of purchaser anonymity.

13/3,AB/25 (Item 3 from file: 275)

DIALOG(R) File 275:Gale Group Computer DB(TM)

(c) 2006 The Gale Group. All rts. reserv.

02112564 SUPPLIER NUMBER: 19907960 (USE FORMAT 7 OR 9 FOR FULL TEXT)

Transactions. (includes related articles on tips and electronic commerce technology) (Web Security) (Internet/Web/Online Service Information)

Young, Robbin

Windows Sources, v4, n11, p193(3)

Nov, 1997

ISSN: 1065-9641 LANGUAGE: English RECORD TYPE: Fulltext; Abstract

WORD COUNT: 2239 LINE COUNT: 00175

ABSTRACT: Electronic commerce scares many consumers, but it is being made safer. It is very unlikely that a credit card number will be stolen as it travels along with other data over the Internet, but it is vulnerable if it is stored on a merchant's server. Users should check sites for security practices and should not use sites that lack posted security policies. The Secure Electronic Transaction (SET) protocol also promises to help improve credit card transactions. Users must install an electronic wallet on their systems, then connect to a SET server operating on the seller's Web site. Another SET server operates at the merchant's bank to pay the bills. SET guarantees users of the authenticity of their trading partners. SET sends only the order to the seller, while the bank receives only the credit card number. The seller never sees the credit card number, and the bank does not